Journées AriNews – 30 mai 2000, ENS Lyon.

Complexité du Calcul du Déterminant d'une Matrice Entière

W. EBERLY (Calgary, Canada), M. GIESBRECHT (London, Canada)
G. VILLARD (CNRS - LMC Grenoble)

http://www-lmc.imag.fr/lmc-cf/Gilles.Villard/
http://www.cis.udel.edu/~caviness/linbox/

Plan de la présentation

1. Algèbre Linéaire : “rappels”

2. Motivations - Complexités de base

3. Idée de la nouvelle démarche

4. Facteurs invariants, perturbations de rang-k

5. Tous les facteurs invariants, l'algorithme

Conclusion

1. Algèbre Linéaire : "rappels"

$\rightarrow$ Déterminant d'une matrice $n \times n$ sur un anneau

$$\mathsf{R} = \mathbb{Z}$$

Asymptotiquement en la dimension,
on suppose que les entiers en entrée sont de taille fixée.

$$A = \begin{bmatrix} 43 & -62 & 77 & 66 & 54 & -5 & 99 \\ -61 & -50 & -12 & -18 & 31 & -26 & -62 \\ 1 & -47 & -91 & -47 & -61 & 41 & -58 \\ -90 & 53 & -1 & 94 & 83 & -86 & 23 \\ -84 & 19 & -50 & 88 & -53 & 85 & 49 \\ 78 & 17 & 72 & -99 & -85 & -86 & 30 \\ 80 & 72 & 66 & -29 & -91 & -53 & -19 \end{bmatrix}$$

$$\det \ A = -222570833995966.$$

Lemme. *La taille du déterminant est en* $O\tilde{}(n)$. $\square$

$$\rightarrow \quad Ax = b$$

$$A = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 6 & 0 \\ 0 & 0 & 0 & 0 & 12 \end{bmatrix}$$

Pour des seconds membres aléatoires

$$b = \begin{bmatrix} -68 \\ -42 \\ -47 \\ -32 \\ 37 \end{bmatrix} \quad \rightarrow \quad x = \begin{bmatrix} -68 \\ -42 \\ -\frac{47}{2} \\ -16/3 \\ 37/12 \end{bmatrix}$$

ou

$$b = \begin{bmatrix} -93 \\ -58 \\ -90 \\ -53 \\ -69 \end{bmatrix} \quad \rightarrow \quad x = \begin{bmatrix} -93 \\ -58 \\ -45 \\ -53/6 \\ -23/4 \end{bmatrix}$$

$Ax = b$, par les règles de Cramer :

$$x_j = N_j / \det\ A$$

$$N_j = \sum_i (-1)^{i+j} b_i\ A \begin{pmatrix} \{1 \dots n\} \setminus \{i\} \\ \{1 \dots n\} \setminus \{j\} \end{pmatrix}$$

$\rightarrow$ Donc si les mineurs $(n-1) \times (n-1)$ ont un *pgcd non trivial* ont n'a qu'un diviseur du déterminant à l'aide des dénominateurs de solutions aléatoires.

Cette notion est complètement comprise à l'aide de la

$\rightarrow$ Forme normale de Smith

$\triangleright$ $A \in \mathbb{Z}^{n \times n}$

$\triangleright$ Equivalence : matrice unimodulaires.

Le déterminant n'est modifié qu'à une unité près.

Théorème. *Toute matrice est équivalente à une matrice diagonale telle que ses éléments diagonaux s_i vérifient*

$$s_i \text{ divise } s_{i+1}.$$

$\square$

C'est la ***forme normale de Smith***.

... un exemple,

$$A = \begin{bmatrix} -92 & 4 & 90 & 2 & 90 & -190 \\ 245 & -11 & -240 & -5 & -239 & 505 \\ 185 & 1 & -180 & 1 & -191 & 362 \\ 308 & -6 & -300 & -2 & -310 & 617 \\ 248 & -6 & -240 & -2 & -250 & 498 \\ 124 & 6 & -120 & 2 & -132 & 231 \end{bmatrix}$$

$$\downarrow$$

$$S = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 6 & 0 \\ 0 & 0 & 0 & 0 & 0 & 30 \end{bmatrix}$$

$$\det A = 2 \times 2 \times 6 \times 30$$

Les éléments diagonaux sont appelés ***facteurs invariants***.

Corollaire. *Le déterminant peut se calculer comme le produit des facteurs invariants.* $\square$

$$\begin{bmatrix} 1 & -5 & 23 & 34 \\ 93 & -464 & 2058 & 3067 \\ 45 & -217 & 388 & 833 \\ 81 & -449 & 5347 & 1914 \end{bmatrix} \qquad \begin{bmatrix} 1 & 19 & 0 & 60 \\ -24 & -455 & 95 & -1345 \\ -63 & -1112 & 8077 & 4259 \\ -36 & -649 & 3191 & 3587 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 20 \end{bmatrix} \qquad \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 10 \end{bmatrix}$$

$$\downarrow \qquad\qquad \downarrow$$

$$Ax = b \qquad\qquad Ax = b$$

Donne le déterminant

Donne le plus grand facteur invariant

Lemme. *Le plus grand facteur invariant peut se calculer par un algorithme probabiliste de coût asymptotiquement celui de la résolution d'un système.* $\square$

2. Motivations
Complexités de base

Le produit de matrice

$$\mathcal{M}(n) = O(n^\omega)$$

$$\left(\subset O(n^{2.376})\right) \qquad\qquad O(n^3)$$

$Ax = b$ sur $\mathbb{Z}$

$\heartsuit$ Résoudre un système linéaire est "bon marché"

`Algorithme` p-adique :

$Ax = b$ se résoud en $\tilde{O}(n^3)$ opérations binaires.

Solution sous la forme $x = x_0 + px_1 + p^2x^2 + \ldots + p^K x_K$

Idée de l'algorithme :

- itératif / exact, correction du résidu,
- un chiffre p-adique à chaque étape,
- $\tilde{O}(n)$ étapes de produits matrice / vecteur.

$$\Downarrow$$

Plus grand facteur invariant

i.e.

diviseur du déterminant

en $\tilde{O}(n^3)$

Précédentes approches pour le déterminant

$\rightarrow$ Un entier de taille $\tilde{O}(n)$ à calculer

- $\tilde{O}(n)$ déterminants modulo p_i,
- reconstruction du déterminant entier.

$$\Downarrow$$

Déterminant en $\tilde{O}(n^{\omega+1})$

Résolution de $Ax = b$
Plus grand facteur invariant

$$\tilde{O}(n^3)$$

Déterminant ?

(précédentes approches pour le déterminant)
Inversion d'une matrice

$$\tilde{O}(n^{\omega+1}), \quad O(n^{3.376}), \tilde{O}(n^4)$$

Plus grand facteur invariant

$$\Downarrow \quad ?$$

Tous les facteurs invariants,
donc le déterminant
donc la forme normale de Smith

Mise en défaut des précédentes approches :

Les facteurs invariants sont $\boldsymbol{tous}$ calculés explicitement.

$$\Downarrow$$

$$\text{“Coût”} \quad \equiv \quad n \times \text{calcul d'1 facteur invariant}$$

3. Idée de la nouvelle démarche

D'abord supprimer la redondance !

Nombre de facteurs invariants distincts ?

Au pire :

$$\begin{bmatrix} 1 & & & & & \\ & 2 & & & & \\ & & 2^2 & & & \\ & & & 2^3 & & \\ & & & & \ddots & \\ & & & & & 2^\mu \end{bmatrix}$$

$$\mu^2 \quad \text{doit être en} \quad \tilde{O}(n)$$

Lemme. *Le nombre de facteurs invariants distincts est en* $\tilde{O}(\sqrt{n})$.

> ▷ **Clef 1.**
> Calculer **seulement** ces facteurs distincts et leurs multiplicités.

On a vu que l'on sait calculer le plus grand facteur invariant,

$\triangleright$ **Clef 2.**
Supposons que l'on sache calculer **n'importe lequel** des facteurs invariants.

$\triangleright$ **Clef 3.**
Recherche binaires des seuils des degrés ou des tailles.

`Premier exemple,`

$$\begin{bmatrix} 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 \end{bmatrix}$$

`Déroulement :`

Calcul du premier facteur invariant, S_1
Calcul du dernier facteur invariant, S_n
$\diamond$ Constat qu'ils sont égaux.

Deuxième exemple,

$$\begin{bmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 \end{bmatrix}$$

Déroulement :

Calcul du premier facteur invariant, S_1

Calcul du dernier facteur invariant, S_n

A la moitié : calcul de $S_{\frac{n}{2}}$ et $S_{\frac{n}{2}+1}$

$\diamond$ Constat de $S_1 = S_{\frac{n}{2}}$

$\diamond$ Constat de $S_{\frac{n}{2}+1} = S_n$

4. Facteurs invariants
Perturbations de rang-k

"La clef manquante"

$\triangleright$ **Clef 2.**
N'importe lequel des facteurs invariants?

Effet d'une perturbation de rang 1 :

$$\begin{bmatrix} (17) & 0 & 0 & 0 \\ 0 & (17) & 0 & 0 \\ 0 & 0 & (17)^2 & 0 \\ 0 & 0 & 0 & (17)^3 \end{bmatrix} + \begin{bmatrix} 3089 & 2304 & 4672 & -2560 \\ -1632 & -1207 & -2482 & 1360 \\ 2880 & 2160 & 4669 & -2400 \\ 4752 & 3564 & 7227 & 953 \end{bmatrix}$$

$$\downarrow$$

la nouvelle forme de Smith :

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & (17) & 0 & 0 \\ 0 & 0 & (17) & 0 \\ 0 & 0 & 0 & (5)\,(17)^2\,(79)\;(1543) \end{bmatrix}$$

Effet d'une perturbation de rang 2 :

$$\begin{bmatrix} (17) & 0 & 0 & 0 \\ 0 & (17) & 0 & 0 \\ 0 & 0 & (17)^2 & 0 \\ 0 & 0 & 0 & (17)^3 \end{bmatrix} + \begin{bmatrix} 526 & -2989 & -2239 & 1245 \\ 1924 & -5177 & -69 & 1980 \\ -3094 & 6664 & -1922 & -2430 \\ 2328 & -7154 & -1279 & 7697 \end{bmatrix}$$

$$\downarrow$$

la nouvelle forme de Smith :

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & (17) & 0 \\ 0 & 0 & 0 & (2)(3)(17)(229)(11608589) \end{bmatrix}$$

`Algorithme` : s_{n-k}?

Calcul de s_n le plus grand fact. inv. de A
B perturbation aléatoire de rang k
$f \leftarrow$ calcul du plus grand fact. inv. de $A + B$
Retourner $\operatorname{pgcd}(s_n, f)$

Exemple pour le troisième facteur invariant :

1. Plus grand : 17^3.
2. Plus grand après perturbation : $17 * 15950201286$.
3. Le troisième : $\operatorname{pgcd}(17^3, 17 * 15950201286) = 17$.

Lemme. *N'importe lequel des facteurs invariants peut se calculer en $\tilde{O}(n^3)$, ou encore, en le coût asymptotique d'une résolution de système.* $\square$

5. Tous les facteurs invariants
L'algorithme

Un facteur

Function InvFact

Input: an index $1 \le i \le n$.
Output: the invariant factor s_i.

Compute the largest inv. fact. s_1 of A and if $i = 1$ return s_1
Choose a random rank $i - 1$ perturbation B
Compute g the largest invariant factor of $A + B$
Return $\gcd(s_1, g)$. $\square$

La recherche binaire des seuils

Function Search

Input: $[(l, f_l), (m, f_m)]$, $l < m$.
Output: $[l_1, \psi_1, \ldots, l_\kappa, \psi_\kappa]$

If $l = m - 1$
    if $f_l = f_m$ then Return $[2, f_l]$
    if $f_l \neq f_m$ then Return $[1, f_l, 1, f_m]$
$k := \lceil (l + m)/2 \rceil$
$f_k :=$InvFact(k)
If $f_l \neq f_k$ then $[k_1, \psi_1, \ldots, k_r, \psi_r] :=$ Search$((l, f_l), (k, f_k))$
    else $r := 1$, $[k_1, \psi_1] := [k - l + 1, f_l]$
If $f_k \neq f_m$ then $[m_1, \tilde{\psi}_1, \ldots, m_s, \tilde{\psi}_s] :=$ Search$((k, f_k), (m, f_m))$
    else $s := 1$, $[m_1, \tilde{\psi}_1] := [m - k + 1, f_m]$
*** Here,* $\psi_r = \tilde{\psi}_1$ ****
Return $[k_1, \psi_1, \ldots, k_r + m_1 - 1, \psi_r, m_2, \tilde{\psi}_2, \ldots, m_s, \tilde{\psi}_s]$. $\square$

Tous les facteurs invariants
Le déterminant comme produit

Algorithm Smith

Input: $A \in \mathsf{K}^{n\times n}$.
Output: the Smith normal form of A.

$f_1 := \mathsf{InvFact}(1)$
$f_n := \mathsf{InvFact}(n)$
$\mathsf{SearchThresholds}(1, f_1, n, f_n)$. $\square$

Déterminant sur $\mathbb{Z}$

$$\tilde{O}(n^4) \qquad\qquad \tilde{O}(n^{\omega+1}) \subset \tilde{O}(n^{3.376})$$

$$\downarrow \qquad\qquad\qquad\qquad \downarrow$$

$$\tilde{O}(\sqrt{n}\; n^3) \qquad\qquad \tilde{O}(n^{2+\omega/2}) \subset \tilde{O}(n^{3.19})$$

Conclusion

Déterminant sur $\mathbb{Z}$

$$\tilde{O}(n^{2+\omega/2})$$

$$\downarrow$$

$$\tilde{O}(n^{\omega}) \quad ?$$

- Méthode par blocs.
- Réduction de la précision [Avnaim et al.].